2014 年 6 月 9 日
株式会社日立製作所

指静脈情報を用いた電子決済向け生体署名システムの試作に成功

なりすましや改ざんを防ぎ、安全・便利な電子決済を実現可能に

株式会社日立製作所(執行役社長兼 COO:東原 敏昭／以下、日立)は、このたび、クレジット決済やオンラインバンキング、企業間電子商取引などの電子決済における取引データの偽造・改ざんを防ぐとともに、より確実な本人確認を実現する、電子決済向け生体署名システムの試作に成功しました。このシステムは、生体情報を秘密鍵として用いる電子署名技術(生体署名技術)を指静脈認証装置*1 に適用したもので、パスワードや IC カードを使わずに指静脈情報のみに基づいて決済ができます。試作システムでは、指静脈情報そのものが秘密鍵となるため、従来厳密な管理が必要であった秘密鍵をユーザー側で保存する必要がありません。また、システムに登録するデータ(公開鍵)から指静脈情報を復元することはできないため、生体情報の漏えいや偽造を防ぎます。これにより、オンラインでのクレジット決済や銀行決済において、電子署名技術に基づくより便利で確実な本人認証を可能にします。

クレジット決済やオンラインバンキング、企業間電子商取引など、インターネットを介した電子決済の規模は拡大の一途をたどっています。しかし一方で、フィッシングや中間者攻撃、MITB(Man-in-the-Browser)*2 などの攻撃手法の高度化に伴い、不正な取引による被害も増加しています。こうした攻撃を防止し安全な電子決済を実現するためには、マルウェア対策などの様々なセキュリティ対策に加えて、PKI*3 に基づく相互認証や、取引情報の改ざん防止が重要となります。しかし、PKI の秘密鍵や署名鍵は、IC カードやハードウェアトークンといったセキュリティデバイスに格納されているため、これをユーザーが安全に管理する必要があります。一方、より便利で確実な本人確認を実現する認証手段として静脈や指紋を使った生体認証が注目されていますが、システムに登録された生体情報が万一漏えいすると、偽造やなりすまし、プライバシー侵害など大きなリスクが発生します。

これに対し日立は、生体情報のように揺らぎを持つデータを秘密鍵とする電子署名技術(生体署名技術)の原理を 2013 年に開発し、その安全性を数学的に証明しました。具体的には、従来の電子署名技術は秘密鍵に全く揺らぎを許さなかったのに対し、本技術は秘密鍵の揺らぎが一定値以下であれば署名処理を正しく実行できます。これにより、生体情報を秘密鍵とする PKI である PBI(Public Biometrics Infrastructure)の実現可能性を示しました。

今回、本技術を指静脈認証装置に適用し、指静脈情報を秘密鍵とする決済向け電子署名システムを試作しました。この試作にあたり、実際の指静脈データから、生体署名技術に適した揺らぎの小さな特徴データを生成する特徴変換技術を開発しました。開発技術の特徴は以下の通りです。

(1)データの揺らぎの最大値を一定に抑える数学的変換

生体情報など、様々な揺らぎのパターンを持つ任意のデータを、L_∞距離空間*4 の上で表現される特徴データへと変換する、数学的変換の理論を開発しました。この理論は、ランダム射影*5 と呼ばれる数学的変換において、空間の距離構造に関するある種の制約を導入したものです。この変換により、元の画像データで部分的に大きな揺らぎがあったとしても、画像全体として類似していれば、変換後の特徴データにおける揺らぎの最大値は小さく抑えることができます。

(2)指静脈画像の性質を考慮した最適化

日立では、指静脈認証に関する長年の研究により、指静脈画像特有の揺らぎについての統計的な性質に関する知見が蓄積されています。これを上記の数学的変換に反映させることで、揺らぎをより小さく抑えることに成功しました。具体的には、指静脈画像を変換した特徴データの揺らぎを最小化するように、ランダム射影を構成する基底ベクトル*6を適切に選択することで、最適化を行いました。

この特徴変換技術を生体署名技術と組み合わせ、指静脈認証装置に実装しました。開発技術をモバイル端末と組み合わせてクレジット決済を想定したシステムを試作し、評価実験を行った結果、他人受入率1/100 万、本人拒否率 0.2%を達成しました。

従来の決済システムでは、IC カードなどに秘密鍵を格納していたため、これを厳重に管理する必要がありましたが、今回の試作システムでは指静脈情報そのものを秘密鍵として使うため、秘密鍵データの保存・管理の必要がありません。また、システムに登録されるデータ(公開鍵)からは、秘密鍵である指静脈情報を復元できないことが、既に数学的に保証されています。このように試作システムでは、従来厳密な管理が必要であった秘密鍵や指静脈情報がユーザー側では保存されないため、秘密鍵や指静脈情報の漏えいや改ざんを防ぎます。これにより PBI を用いた安全・便利な決済認証の実現の可能性を示しました。

今後、日立は指静脈認証装置と PBI を活用した次世代決済認証について、将来の実用化に向けたさらなる技術開発を進めていきます。

本システムの試作にあたっては、株式会社ジェーシービー(代表取締役兼執行役員社長:川西 孝雄)より、PBI 技術のクレジット決済適用における有効性などの知見を得て、実施しました。

なお、本システムは、2014 年 6 月 11 日に東京コンベンションホールにて開催される「日立セキュリティソリューションセミナー」にて参考展示する予定です。

*1 指静脈認証装置:日立指静脈認証装置 H-1,S-1
*2 MITB:利用者の PC に感染したマルウェアが、ブラウザと利用者の間に割り込み、取引内容を改ざんする攻撃。
*3 PKI:Public Key Infrastructure(公開鍵基盤)とは、公開鍵暗号技術に基づいて、電子認証、電子署名、暗号の機能を提供する情報セキュリティ基盤のこと。
*4 L_∞距離空間:2 つのベクトル間の距離が、各要素の差分の最大値で定義される空間。L_∞空間上での距離が近いということは、ベクトル間の誤差の最大値が小さいことを意味する。
*5 ランダム射影:ランダムに選択された基底ベクトルへの射影に基づく線形変換。ランダムに選択された基底ベクトルへの射影に基づいて、あるベクトル空間から別のベクトル空間へ変換すること。
*6 基底ベクトル:ランダム射影の具体的な変換式を決定するパラメータ。

■照会先

株式会社日立製作所 横浜研究所 企画室[担当:吉田]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話 050-3135-3409 (直通)

以 上